9 Anwendungsschicht

9.1 Architektur der Anwendungsprotokolle im Internet
9.2 smpt für elektronische Post
9.3 ftp für Dateitransfer
9.4 nfs für den Fernzugriff auf Dateien im Netz
9.5 telnet für virtuelles Terminal (remote login)
9.6 http für das World Wide Web
9.7 Telefondienste über IP

9.1 Architektur der Anwendungsprotokolle im Internet

<table>
<tr><td>SMTP
Mail</td><td>FTP
File Transfer</td><td>TELNET
Remote
Login</td><td>NFS</td></tr>
<tr><td colspan="3">TCP</td><td>UDP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td colspan="4">LLC und MAC</td></tr>
<tr><td colspan="4">Bitübertragungsschicht</td></tr>
</table>

SMTP	=	Simple Mail Transfer Protocol
FTP	=	File Transfer Protocol
TELNET	=	Remote Login Protocol
UDP	=	User Datagram Protocol
NFS	=	Network File System
TCP	=	Transmission Protocol
IP	=	Internet Protocol
LLC	=	Logical Link Control
MAC	=	Media Access Control

9.2 smpt für elektronische Post

smtp: Simple Mail Transfer Protocol

- Electronic Mail im Internet
- Benutzt im Gegensatz zu X.400 von ITU-T eine direkte Verbindung zum Ziel-Host (kein Mail Forwarding in Schicht 7)
- TCP-Port: 25

- Protokoll-Elemente:

HELO	Vorstellung
MAIL	Angabe des Absenders
RCPT	Angabe des Empfängers
DATA	Senden der Nachrichten
QUIT	Ende
VRFY	Verifizieren des Benutzernamens
EXPN	Angabe von Verteilerlisten

- Zu smtp existieren zahllose graphische Benutzeroberflächen

Funktionalität von smtp

- Das smtp-Protokoll sorgt nur für die Übertragung der Nachrichten, nicht aber für die Entgegennahme, Speicherung oder Präsentation der Nachricht ("local matter")
- Die Mailer-Instanzen kommunizieren mittels lesbarem Text (ASCII)
- Empfänger muß jede Meldung bestätigen
- Mehrere Nachrichten (mails) können nacheinander über eine TCP-Verbindung geschickt werden, wenn die Empfänger auf demselben Host sind
- Weiterleitung von Nachrichten (forwarding) bei einer Adressenänderung des Benutzers möglich

Beispiel-Interaktion:

```
R:    220 Beta.GOV Simple Mail Transfer
      Service Ready
S:    HELO Alpha.EDU
R:    250 Beta.GOV

S:    MAIL FROM:<Smith@Slphs.EDU>
R:    250 OK

S:    RCPT TO:<Green@Beta.GOV>
R:    550 No such user here

S:    RCPT TO:<Brown@Beta.GOV>
R:    250 OK

S:    DATA
R:    354 Start mail input; end with
      <CR>LF>.<CR><LF>
S:    ...sends body of mail message...
S:    ...continues for as many lines as
      message contains
S:    <CR><LF>.<CR><LF>
R:    250 OK

S:    QUIT
R:    221 Beta.GOV Service closing trans-
      mission channel
```

9.3 ftp für Dateitransfer

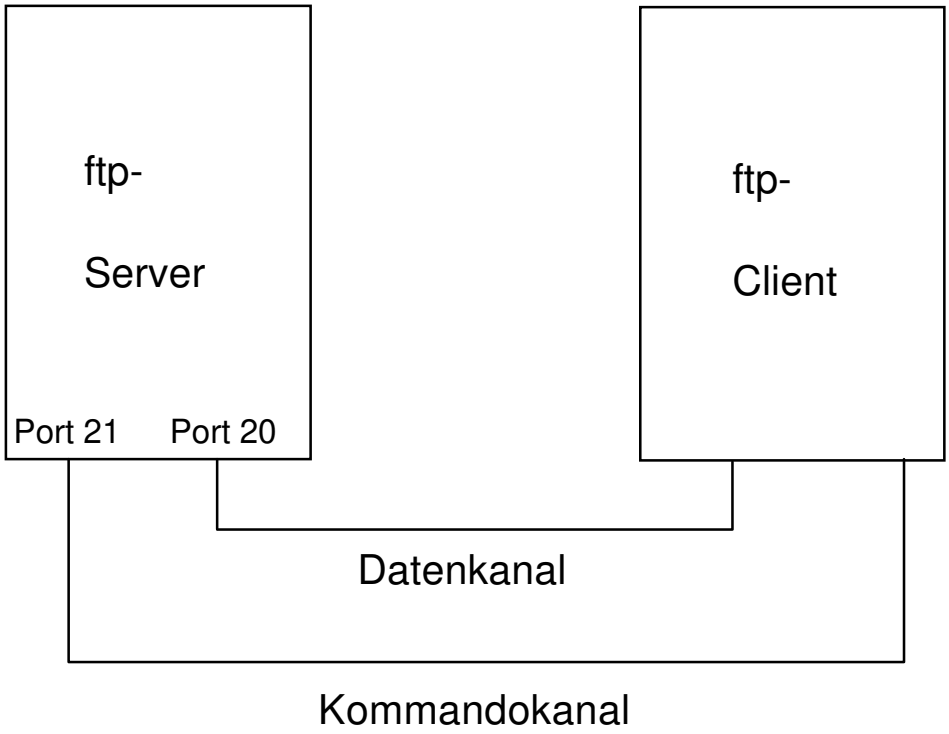
ftp (file transfer protocol)
tftp (trivial file transfer protocol)

ftp erlaubt

- das Senden, Empfangen, Löschen und Umbenennen von Dateien
- das Einrichten und Löschen von Verzeichnissen
- den Wechsel des aktuellen Verzeichnisses

Die Dateiübertragung kann in binärem oder ASCII-Modus erfolgen. Im binären Modus (auch "image file type" genannt) wird der Bitstrom aus dem Speicher des Senders ausgelesen und unverändert übertragen. Im ASCII-Modus geht ftp davon aus, daß nur alphanumerische Zeichen übertragen werden sollen. Als Transfercodierung wird ASCII gewählt; wenn der Sender oder der Empfänger eine andere lokale Darstellung hat, wird umcodiert. Im Transfer wird ein Zeilenende als <CR><LF> codiert; wenn der Sender oder der Empfänger eine andere lokale Darstellung dafür hat, wird auch hier umcodiert. Der ASCII-Modus implementiert also eine minimale Funktionalität der Darstellungsschicht für Textdateien.

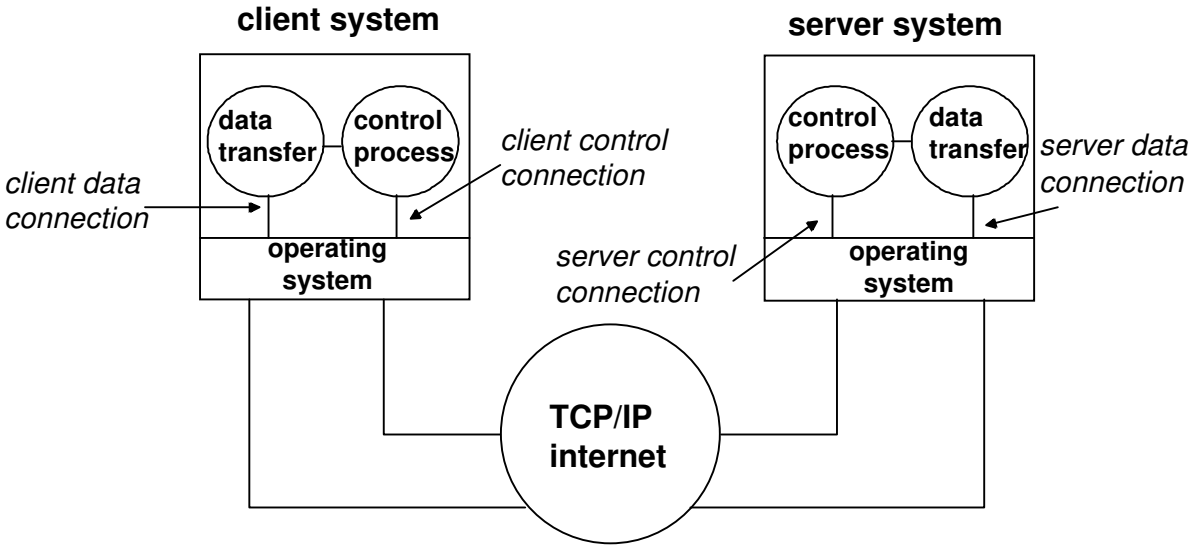
Grundlagen von ftp



- Die Kommandos von ftp werden als vierbuchstabige Zeichenfolge plus Optionen übertragen (z.B. PASS xyz)
- Als Antwort wird eine Folge von 3 Ziffern geliefert, die erste davon gibt über den Typ der Antwort Auskunft (1,2,3 => kein Fehler, 4,5 => Fehler usw.)

Architektur von ftp

- Der ftp-Client läuft als Programm im Adreßraum des Benutzers
- Keine Integration in das lokale Dateisystem (keine Transparenz des Datei-Speicherorts)



- separate Verbindung (TCP) für Kontrolle und Daten
- Authentifizierung (Password) beim Aufbau der Kontrollverbindung
- Directory-Operationen (*ls, cd, rm,* ...)
- put und get zum Kopieren von Daten
- help-Funktionen

9.4 nfs für den Fernzugriff auf Dateien im Netz

Geschichte

1984:	Ankündigung
1985:	Erstes Produkt auf einer SUN
1986:	Portierung für System-V-release-2
1986:	NFS 3.0: (verbessertes YP) und PC-NFS
1987:	NFS 3.2: File-Locking
1989:	NFS 4.0: Verschlüsselung
1989:	Lizensierung durch 260 Hersteller

Merkmale von nfs

- Transparenter Zugriff auf Dateien in entfernten Dateisystemen
- integriert in das Betriebssystem/Dateisystem
- entwickelt seit 1985 von SUN Micro-Systems
- inzwischen Standard auf nahezu allen UNIX-Rechnern (z.T. auch DOS: PC-NFS)
- offenes System (Spezifikation ist öffentlich)
- eignet sich für heterogene Netzwerke
- Portierung ist einfach
- Referenzimplementierung ist öffentlich
- billig
- Bestandteil von UNIX-V-Release-4 seit Dezember 1989
- PC-NFS für PC's
- Implementierungen für VMS und MVS
- Knoten importieren / exportieren Directories
- Client / Server-Modell
- Kommunikation über UDP, also verbindungslos
- keine Darstellungsdienste, nur Lesen und Schreiben von Byte-Strömen

Mounting

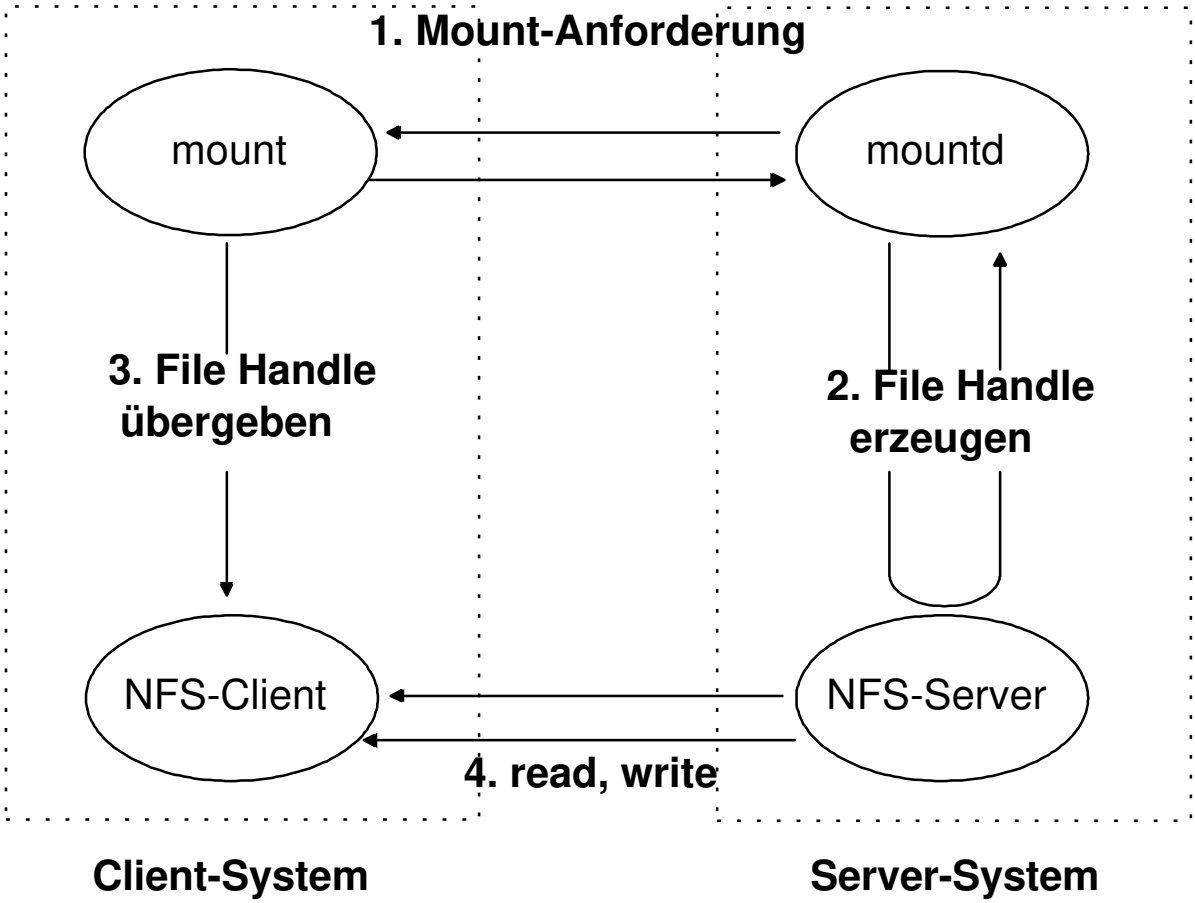
Das NFS-Protokoll ist lediglich ein Protokoll für den Dateizugriff (Lesen und Schreiben). Das Bereitstellen von entfernten Dateien geschieht durch das mount-Protokoll.

mount verbindet ein entferntes Datensystem mit einem lokalen Verzeichnis, d.h. der gesamte entfernte Dateibaum wird in das bisherige Verzeichnis eingehängt.

Danach kann über NFS auf die entfernten Dateien wie auf lokale Dateien zugegriffen werden.

mount und nfs sind getrennte Protokolle, mount bzw. mountd stellen lediglich einige Informationen für nfs bzw. nfsd zur Verfügung (z.B. Rechnernamen und Pfad).

NFS-Protokoll und MOUNT-Protokoll



mountd und nfsd (demons im Unix-Sinne) werden beim Hochfahren des Servers automatisch gestartet. nfsd aktiviert den NFS-Server-Code im Betriebssystem.

Beim MOUNT-Vorgang wird auf der Server-Seite ein "File Handle" (eindeutiger Dateisystem-Kontrollblock) erzeugt und an den Client zurückgegeben. Der NFS-Client verwendet diesen bei allen späteren Zugriffen auf den entfernten Verzeichnis(-teil)-Baum.

NFS und Sicherheit

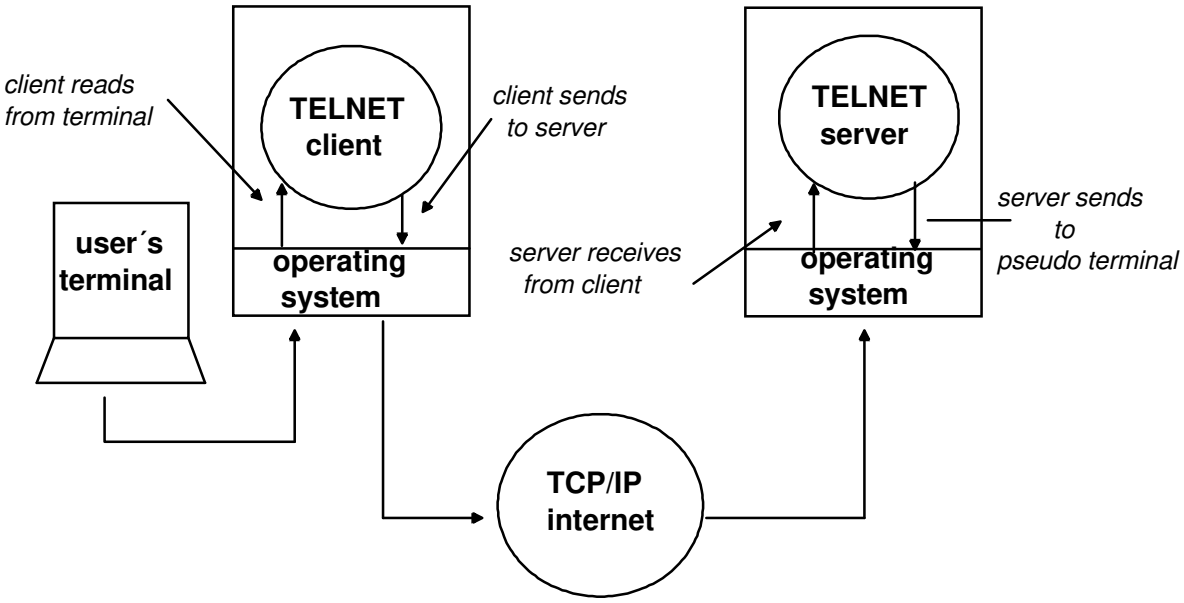
- Anschluß an Netz ist immer potentielles Sicherheitsloch
- Ethernet-Pakete lassen sich abhören
- Ab Version 4.0: Verschlüsselung in NFS unterstützt
- Datenzugriff nur von privilegierten Ports (<1024) erlaubt (Variable nfs_portmon im Kernel)
- Ähnlicher Mechanismus existiert für mount
- Vergleich Internet-Adresse, Client-Name mit /etc/hosts

Lock-Manager

- Problem: gleichzeitiger Schreibzugriff durch mehrere entfernte NFS-Clients
- Der Lock-Manager ermöglicht das Sperren von Dateien
- Dienst parallel zu NFS (lockd)
- erst ab NFS 3.2
- im SunOS nicht Teil des Betriebssystems
- Keine Deadlock-Erkennung

9.5 telnet für virtuelles Terminal (remote login)

- Virtuelles Terminal auf einen entfernten Rechner
- alphanumerisch, full screen mit Scrolling, Blinken etc. Also mächtiger als der PAD von X.25, aber nicht grafikfähig wie X. 11
- setzt auf TCP auf



TCP-Verbindung zwischen Client und Server

9.6 HTTP für das World Wide Web

HTTP - Entwurfsziele

- Einfaches request/response- Protokoll, ASCII-Format
- Minimale Transaktionsbelastung des Servers: zustandsloses Protokoll
- Für jedes einzelne Dokument wird eine Verbindung aufgebaut und wieder geschlossen, Serverprozeß belegt dann keine Ressourcen mehr.
- Caching von DNS-Informationen (Client Caching)
- Übertragung über ein zuverlässiges Transportprotokoll, typischerweise TCP/IP, andere Protokolle durchaus denkbar

HTTP (Fortsetzung)

Historie

- 1989: HTTP 0.9 ausschließlich für Hypertext konzipiert
- 1990: HTTP 1.0 Übertragung beliebiger Datenformate
- 7/1993: HTTP Internet Draft, erste Fassung
- 1996: HTTP 1.0 siebte Fassung; Inform.RFC
- 4/1996: HTTP 1.1 in Entwicklung (Internet Draft)
- 1997: HTTP NG (inkompatibel)

HTTP-Transaktion

1. Verbindungsaufbau

- WWW-Client baut eine TCP/IP-Verbindung zum WWW-Server auf
- TCP-Port 80

2. Anforderungen (Request)

- Client sendet Request über aufgebaute Verbindung (i.d.R. GET, PUT, POST)

3. Antwort (Response)

- Reaktion des Servers auf Request, z.B. angefordertes Dokument
- Code über Status des Requests

4. Verbindungsabbau

- nach Übertragung Beendigung der Verbindung durch Server
- Datenübertragung stets mit 8 Bit/Zeichen

Beispiel: ASCII-Kommunikation von http

	bash$ telnet numalfix 80 Trying... Connected to numalfix.wifo.uni-mannheim.de Escape character is '^]'.	*Leerzeile*
Client: Request	**GET /index.html HTTP/1.0** **Accept: image/gif**	*Methode*
Server: Response	HTTP/1.0 200 Document follows Date: Sun, 09 Jun 1996 13:13:09 GMT Server: NCSA/1.5 Content-type: text/html Last-modified: Thu, 30 May 1996 10:42:31 GMT Content-length: 1751 <html><head><title>BWL-Hauptseite</title><head> <body> ... <IMG SRC=/images/unilogo.gif... <IMG SRC=/images/FakBWL2.gif... <IMG SRC=/images/ball.red.gif... ...	*Dokumentkopf*

Auszug aus dem Access-Log des WWW-Servers

```
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/index.html HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/neu2.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/FakBWL2.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/unilogo.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/ball.red.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/ball.green.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/minfo.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/minfo.gif HTTP/1.0" 200
obelix.wifo.uni-mannheim.de - - [Datum]
            "GET/images/mup.gif HTTP/1.0"304
```

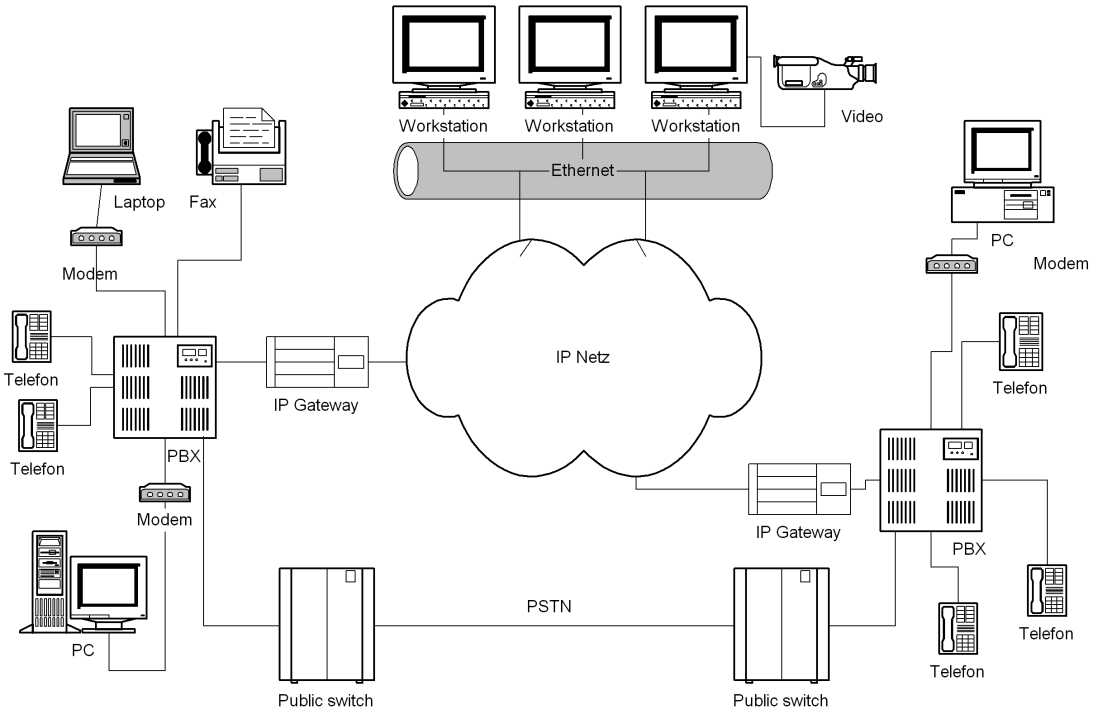
Verbesserungen

- TCP-Verbindung halten, wenn mehrere Dateien vom selben Server zu holen sind (möglich ab HTTP 1.1)
- Aufbau mehrerer paralleler TCP-Verbindungen zur Beschleunigung der Datenübertragung

9.7 Telefondienste über IP*

9.7.1 Grundlagen und Protokolle

- Mehr Funktionalität als herkömmliche Telefonie im leitungsvermittelten Telefonnetz (PSTN)
- Effiziente Realisierung, da Paketvermittlung weniger Overhead und mehr Flexibilität bringt
- Ziel: Multimediakommunikation und intelligente Dienste in IP-basierten Netzen.



*Ich danke Robert Denda und Dr. Andreas Grebe für die Überlassung von Folien für Kapitel 9.7

Gründe für IP-Telefonie

- Herkömmliches Telefonnetz: verbindungsorientiert, leitungsvermittelt, aufwendige Vermittlungsanlagen (PBXs)
- IP-Telefonie:
  - paketvermittelt, statistischer Multiplexeffekt, „einfache“ Router
  - geringere Bandbreite durch Audiokompression (z.B. G.723.1 nur 5,3-6,3 kBit/s gegenüber 64kBit/s bei ISDN)
- Flexibilität bei der Signalisierung
- Integration von Multimedia
- Erweiterbarkeit um intelligente Netzwerkdienste (Anrufweiterleitung, Anklopfen, Mehrpunkt-Verbindungen)
- Skalierbarkeit der Kommunikationsdienstgüte
- Endgerätevielfalt: PCs, Telefone, Fax, etc.
- Nutzung bestehender Datennetze

Motivation für den Anwender:

- Kostenvorteile
- PC-Integration ist oft praktisch

Anforderungen an IP-Telefonie (1)

Hauptproblem: Dienstgüte

- Verzögerung (Delay):
  Experimentell gemessene Verzögerungen:
  - Kodierungs-/Dekodierungsverzögerung:
    ca. 30 ms (G.729A) – 82 ms (G.723.1)
  - Netzwerkverzögerung (Übertragung, Routing, etc.):
    Gateway-Gateway: 30-100 ms
    PC-PC: 50-140 ms
  - Zugriffsverzögerung (Betriebssystem, Sound-und Videokarten, DSPs, ...):
    Gateway-Gateway: 40-80 ms
    PC-PC: 100-340 ms
    Aber: menschliches Ohr sehr sensibel, wünschenswertes Delay: < 100 ms
- Bandbreite
- Paketverlust: FEC erforderlich, erhöht Verzögerung und Datenrate
- Multicast, Heterogenität der Teilnehmer, Dynamic Join-and-Leave erfordern aktive, adaptive QoS-Mechanismen im Netz

Anforderungen an IP-Telefonie (2)

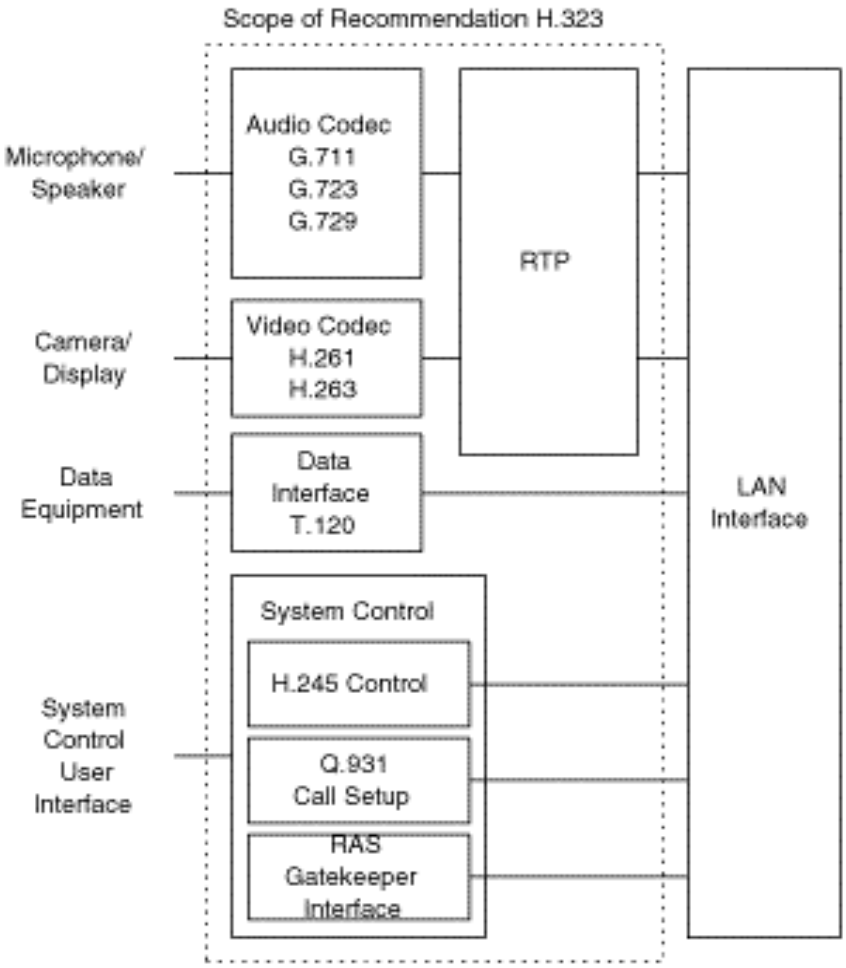
Zusätzlich viele weitere Probleme:

- Crosstalk, Echo, Rauschen (wie bei POTS)
- Leitwegänderungen
- QoS-basierte Gebühren, etc.

- Intelligente Dienste
  - „Standard“ IN/AIN-Dienste: Anklopfen, Anrufbeantworter im Netz, etc.
  - Neue intelligente Dienste:
    Directory-Dienste
    WWW-Schnittstellen u.v.m. ...
- Signalisierung
  - Leichtgewichtige Signalisierung (Internet vs. IN/AIN)
  - neue Medien, erweiterte Dienste, Charging erfordern neue Signalisierungsmechanismen
- Mobilität, Interworking
  - Interworking of LAN, ATM, breitbandige Zugangsnetze, Wireless LAN/WAN
- Sicherheit
- Abrechnungssystem (charging, accounting)

IP-Telefoniestandards und -protokolle

ITU Recommendation H.323

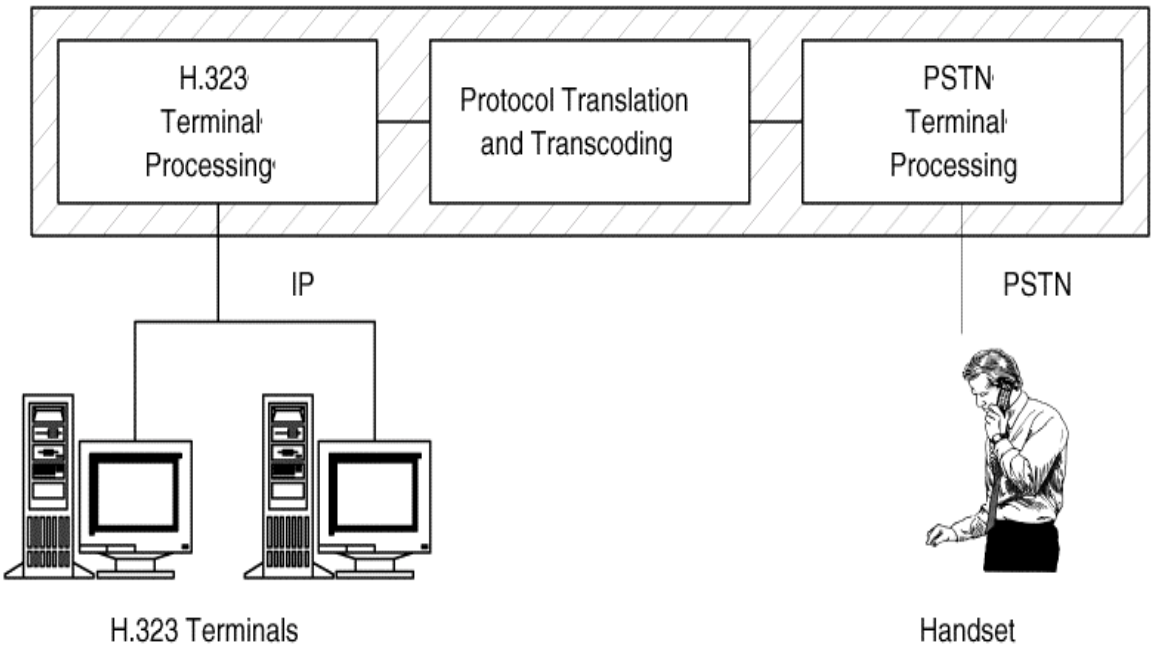


H.323 ist Teil der Kommunikationsstandards H.32x für Videoconferencing. H.323 umfaßt mehrere ITU-Standards für Multimediakommunikation in LANs ohne garantierte Dienstgüte (TCP/IP, IPX (Ethernet), Fast Ethernet und Token Ring).

IP-Telefoniestandards und -protokolle (2)

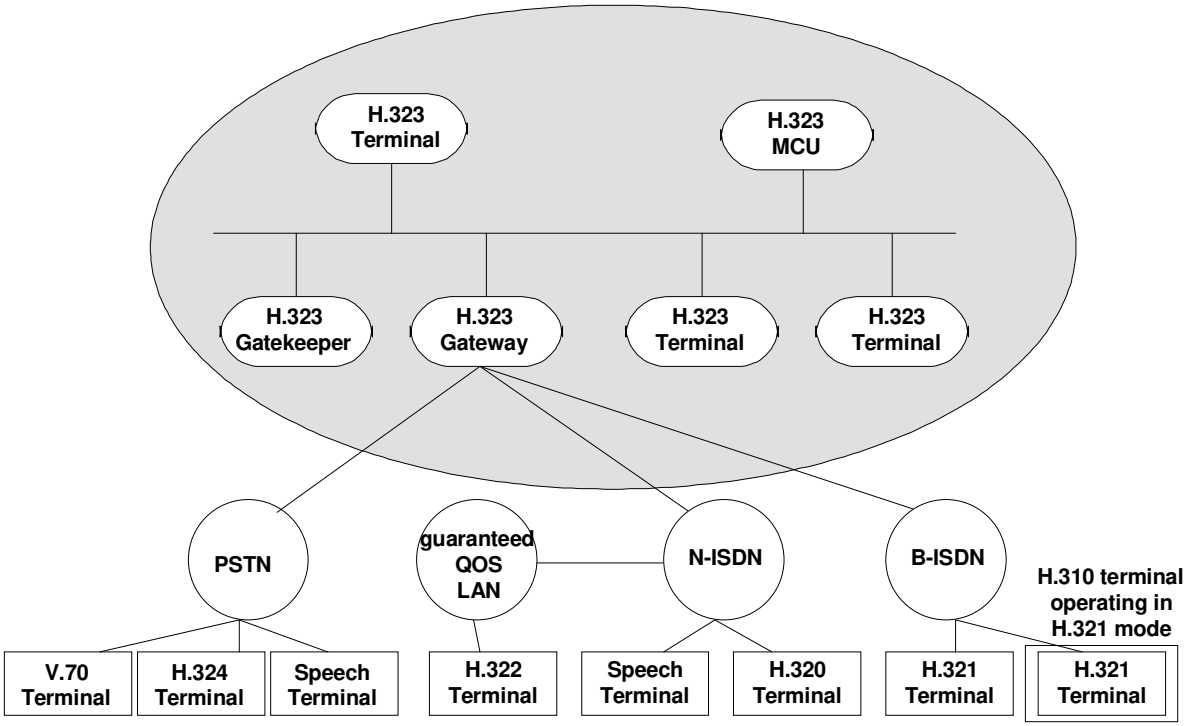
Version 1 von H.323 wurde 1996 verabschiedet, Version 2 im Januar 1998. Version 3 ist geplant.

H.323 wird von den meisten Produkten für Voice-over-IP (VOIP) unterstützt und schließt sowohl herkömmliche Telefongeräte als auch Workstations ein.



H.323 umfaßt Call Control, Multimedia- und Bandbreitenmanagement und definiert die Schnittstellen zwischen LANs und anderen Netzen.

IP-Telefoniestandards und -protokolle (3)



MCU= Multipoint Control Unit
N-ISDN= Narrowband ISDN
B-ISDN= Broadband ISDN

IP-Telefoniestandards und -protokolle (4)

Signalisierungsprotokolle

- Control Protocol for Multimedia Communication (H.245): Ende-zu-Ende-Signalisierung, sehr komplex
- Session Initiation Protocol (SIP): einfaches textbasiertes Signalisierungsprotokoll für Internetkonferenzen und –telefonie, unterstützt u.a. transparente Abbildung von Namen auf Adressen und Rufumleitung
- Digital Subscriber Signalling System No.1 (DSS1 Q.931), Q.93B, Q.932: ISDN-Signalisierung
- RSVP – Resource ReSerVation Protocol: Empfängerorientiertes Protokoll zur QoS- und Bandbreitenreservierung

IP-Telefoniestandards und -protokolle (5)

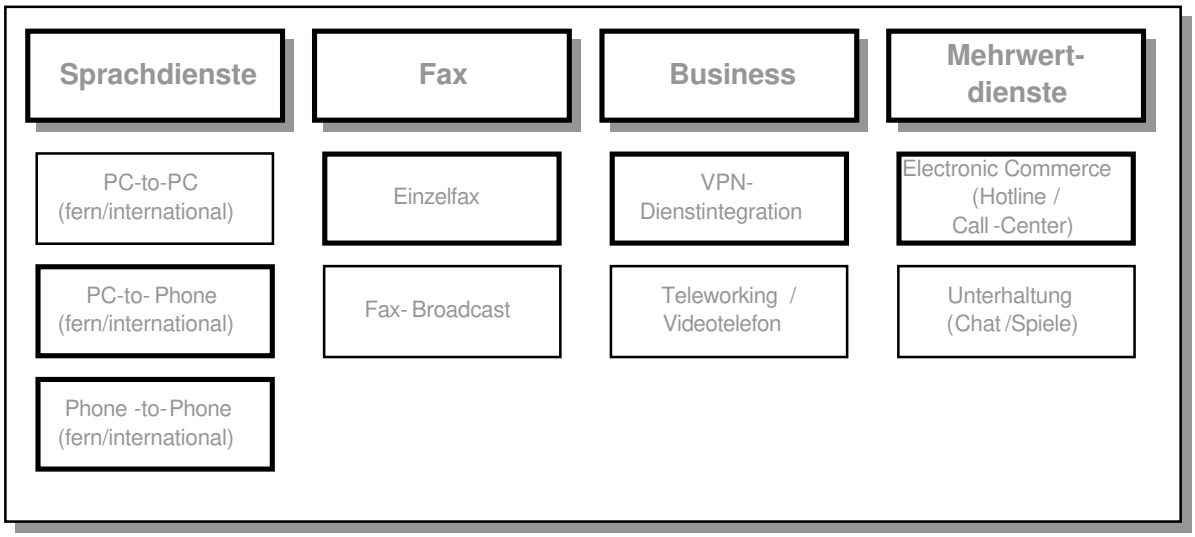
Medienstrom-Kontrollprotokolle

- Real Time Protocol (RTP) / Real Time Control Protocol (RTCP): unterstützt Multimediakommunikation in Echtzeit. Profile werden definiert für verschiedene Payload-Typen (z.B. MPEG-1, H.263)
- Real Time Streaming Protocol (RTSP): erlaubt bidirektionale Übertragung basierend auf RTP, beinhaltet Sicherheitsmechanismen

Netzwerkintelligenz

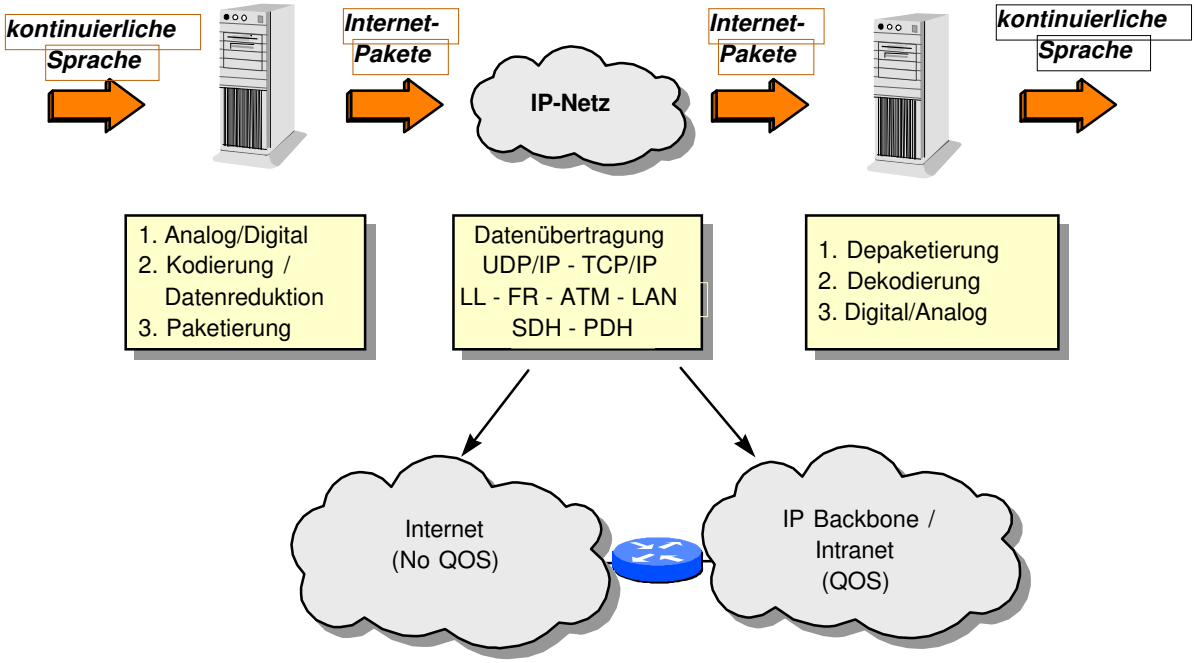
- PSTN: Intelligent Network (IN), Advanced Intelligent Network (AIN)
- IP-Telefonie: Telecommunication Information Networking Architecture (TINA)
- Bereich aktueller Forschung: Nutzung moderner verteilter Systeme (CORBA, Java RMI, DCOM), aktiver Netze und mobiler Agenten zur Implementierung von Netzwerkintelligenz

9.7.2 Voice-over-IP (VOIP)



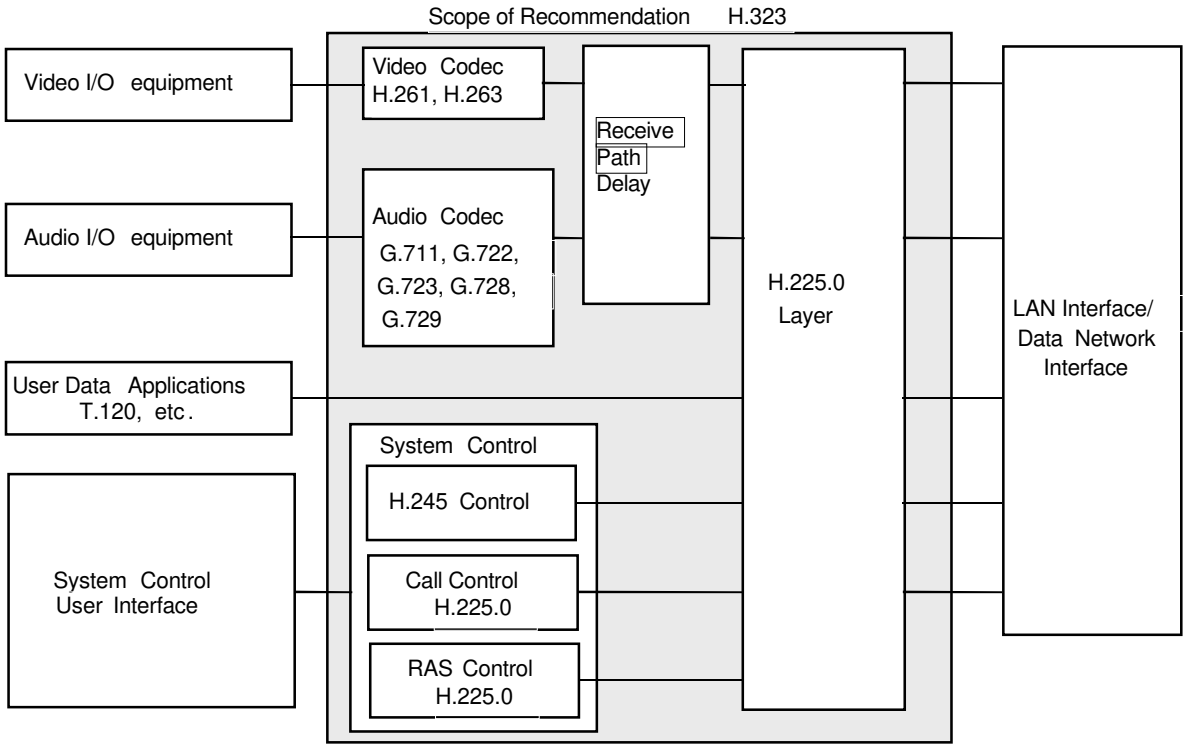
- VOIP-Dienste sind Mehrwertdienste für Internet-Dienstanbieter
- Mittelfristig: Dienstekopplung IP-PSTN

Prinzip von Voice-over-IP (VOIP)



- VOIP heute: nutzbar, einige kommerzielle Dienste, setzt auf Standard-IP auf ("best effort")
- VOIP morgen: gute Qualität (QoS), internationale Dienste/Allianzen

VOIP Signalisierung – H.323



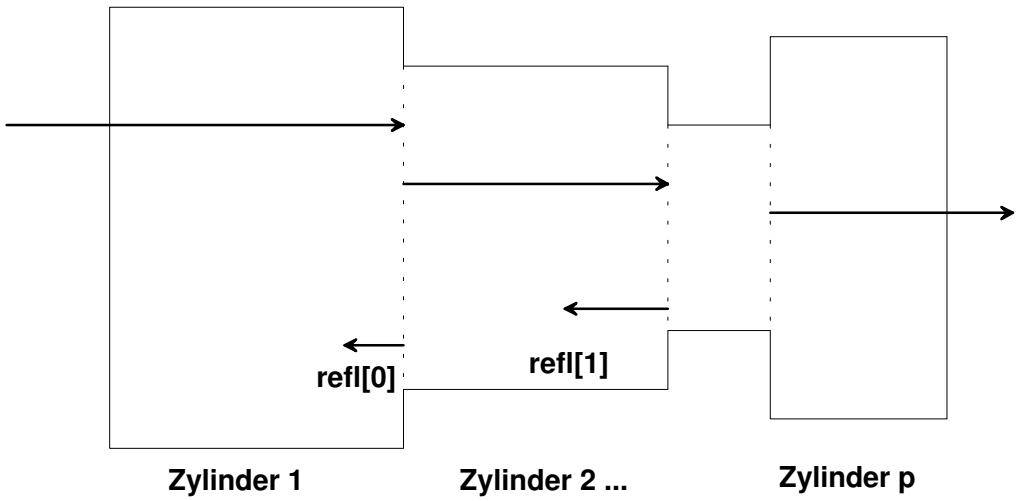
- Heute minimale Interoperabilität durch H.323
- Aktuelle Entwicklungen in Richtung PBX-Vernetzung und öffentliche Vermittlungssysteme (DSS1, SS #7)

Sprachkodierung

IP-Telefonie: Sprachkodierer mit relativ guter Qualität bei sehr niedriger Bitrate (z.B. GSM 06.10 mit 13,2 kBit/s oder G.723.1 mit 5.3 kBit/s - 6.3 kBit/s)

Verwendete Verfahren basieren meist auf Linear Predictive Coding (LPC):
Für jeden Rahmen von Sprachsamples s[ ] werden p Gewichte lpc[0], .. , lpc[p-1] berechnet, so daß für alle Samples s[i] gilt:
s[i] wird möglichst gut durch
lpc[0] * s[i-1] + lpc[1] * s[i-2] + ... + lpc[p-1] * s[i-p]
angenähert (üblich: p=8 oder 14).

Dies entspricht einem analytischen Modell des menschlichen Sprachorgans als System von miteinander verbundenen, verschieden großen Zylindern:



Kodierungsmodell

Akustische Wellen durchlaufen System von Zylindern, werden an Übergängen von Zylindern mit unterschiedlichem Durchmesser teilweise reflektiert und interferieren somit mit nachfolgenden Wellen. Die Reflektionsrate wird durch die Reflektionskoeffizienten refl[0], ..., refl[p-1] repräsentiert. Diese entsprechen nahezu den lpc-Koeffizienten.

Kodierung: Für jeden Rahmen:

1. Berechnung der lpc/refl-Koeffizienten.
2. Ein synthetisch generiertes Signal dient als Eingabe des Modells und ergibt synthetische Sprache.
3. Unterschiede ε_i zwischen synthetischer Sprache und Samples werden kodiert (ε_i klein bei stimmhaften Phonemen); lpc/refl-Koeffizienten werden kodiert.

G.723.1: Adaptiver CELP (Code Excited Linear Predictor) Kodierer:

CELP: ε_i werden als Indizes in ein Codebook kodiert

ACELP: wie CELP, aber Codebook adaptiv

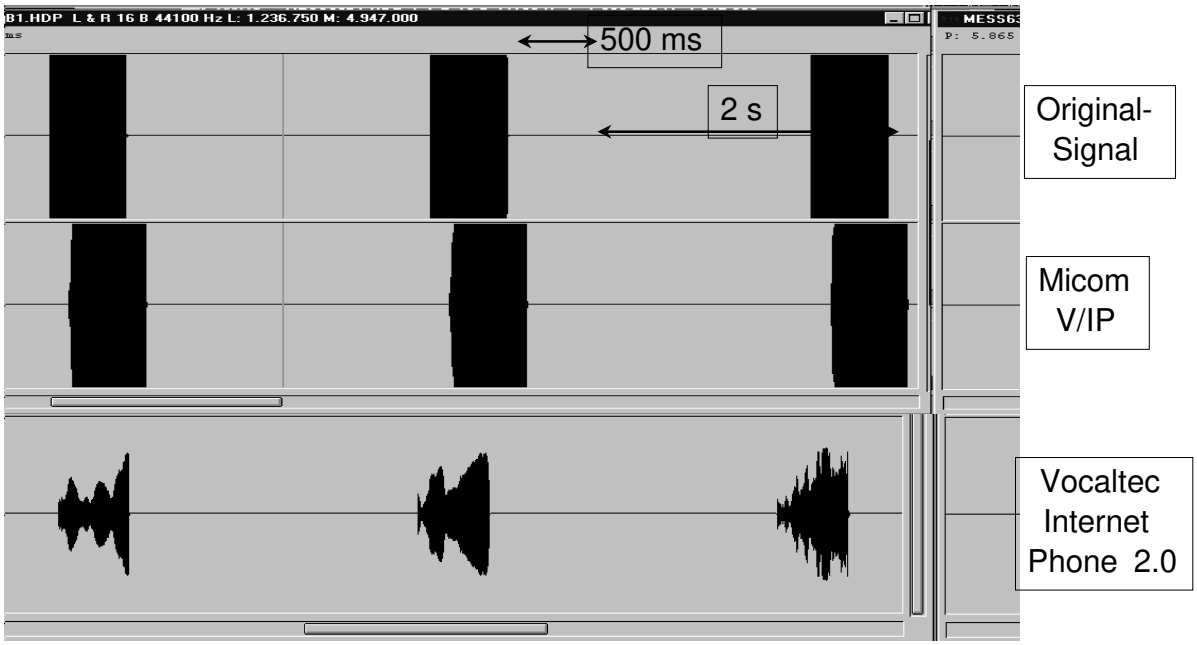
GSM 06.10: Regular Pulse Excitation – Long Term Prediction (RPE-LTP) Kodierer:

Vergleich verschiedener VOIP-Codecs

Codec	Technik	Bitrate	Qualität (MOS)	Standard	Einsatz	Codier-Delay	Leistungs-verbrauch (100 MHz Pentium)
G.711	PCM	64 kbit/s	4,0	H.323	ISDN	< 1 ms	< 1%
G.723.1	ACELP MP-MLQ	5,3 kbit/s 6,3 kbit/s	3,88 3,88	H.324/H.323	PSTN Videotelefon Voice over IP	97,5 ms 97,5 ms	35-49% 35-49%
G.728	LD-CELP	16 kbit/s	3,93	H.323	Voice over IP	3 ms	ca. 65%
G.729	CS-ACEL	8 kbit/s	3,90	H.323	Voice over IP Frame Relay ATM	35 ms	ca. 50%
GSM 6.10	RELP	13 kbit/s	3,80 at 0% errors	not included in H.323	Mobil	ca. 40 ms	real-time coding at 486PC 66MHz
Lucent SX7300P	CS-ACEL	7,3 kbit/s	3,88	not included in H.323	Voice over IP	35 ms	ca. 13,5%

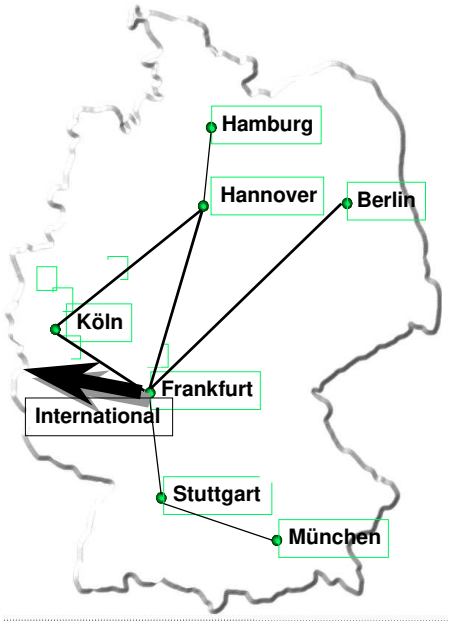
- Mean Opinion Score (MOS)
  Befragung von Testpersonen:
  >3.8 akzeptabel
  >4.0 sehr gute Qualität

Verzerrungen der VOIP-Codecs



- Codecs zeigen sehr stark variierende Verzerrungscharakteristika
- Psycho-akustische Codecs zeigen deutlich stärkere Verzerrungen
- Mean Opinion Score (MOS) in beiden Fällen akzeptabel

Beispiel: VOIP-Testnetz von o.tel.o



Pilotversuch

Berlin, Frankfurt, Hamburg, Hannover, Köln, München, Stuttgart

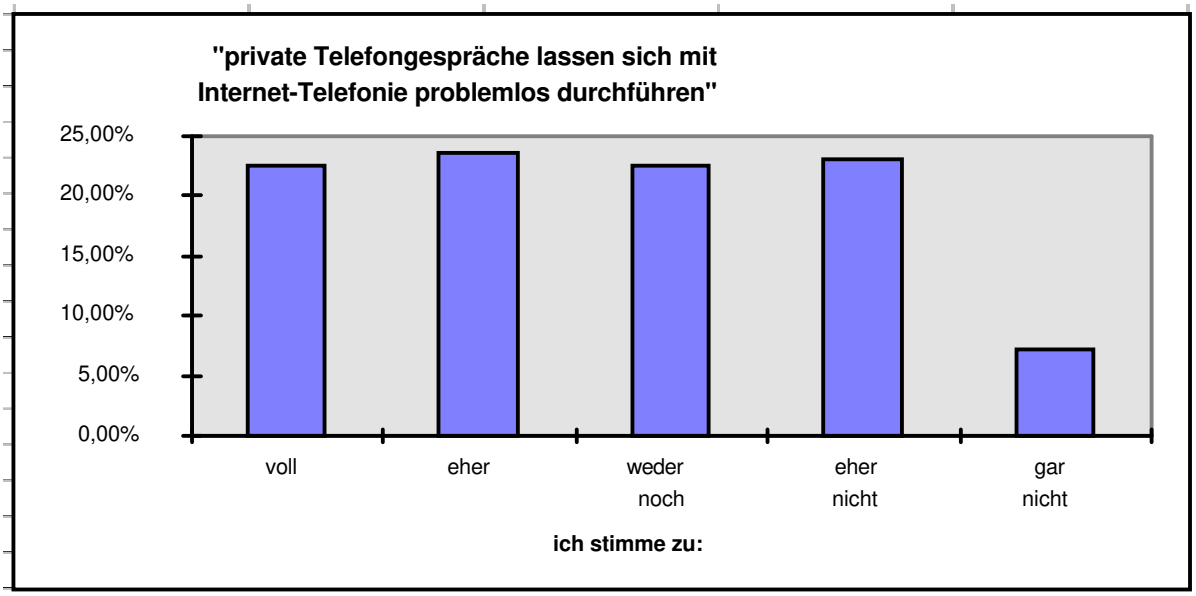
- Kosten:
  IP-Access (entfernungsabhängig)
  + VOIP-Tarif (national / international)
- Labortests seit Mai 1997
- Test mit Endnutzern seit Februar 1998

Endgültiges Dienstangebot

- National flächendeckend
- Kosten:
  IP-Access (entfernungsabhängig)
  + VOIP-Tarif (national / international)
- Service ab Ende 1998

9.7.3 Akzeptanz und Marktpotential

Resonanz privater VOIP-Nutzer



Mehrheit der Testteilnehmer akzeptiert die angebotene Qualität für private Telefonate.

Akzeptanz von VOIP-Diensten

- Privatkunden (Phone-to-Phone)
  - 68% würden VOIP-Dienste nutzen
  - geringere Qualität als ISDN (~GSM) wird akzeptiert

- Businesskunden (Phone-toPhone)
  - 28% würden VOIP-Dienste uneingeschränkt nutzen
  - 65% würden VOIP-Dienste im Intranet einsetzen
  - höhere Qualitätsansprüche im Außenverhältnis (Kunden)

- 52% Kostenreduktion zur Deutschen Telekom werden erwartet (Stand: Oktober 1998)

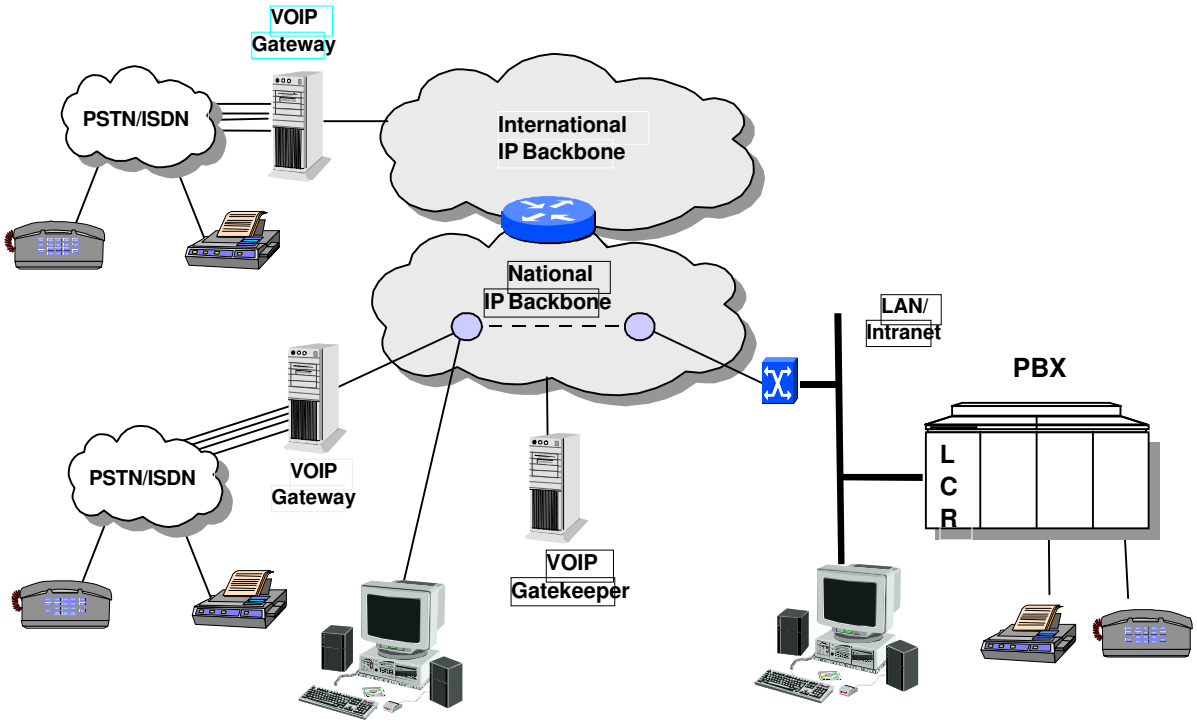
Potentiale für VOIP-Dienste

- Massenmarkt
  - (Phone-to-Phone) (evtl. reguliert)
  - PC-to-Phone (Online-Dienste, Always Online)

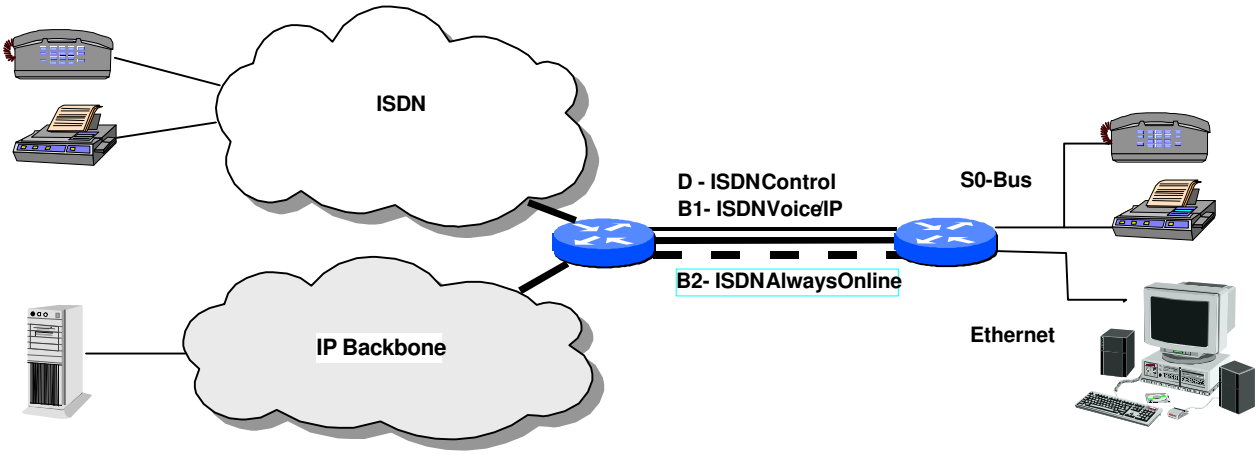
- Geschäftskundenmarkt
  - Intranet/VPN (Virtual Private Network) mit Integration von Fax, Sprache, Daten, Konferenz
  - Internationale Dienste

- VOIP-Mehrwertdienste
  - Click & Call / Web Call Center: Integration von Web, Telefondienst und CallCenter
  - Unified Messaging/Unified Access: universelle Erreichbarkeit inklusive globalem IP Roaming

Potential I: Intranet/VPN

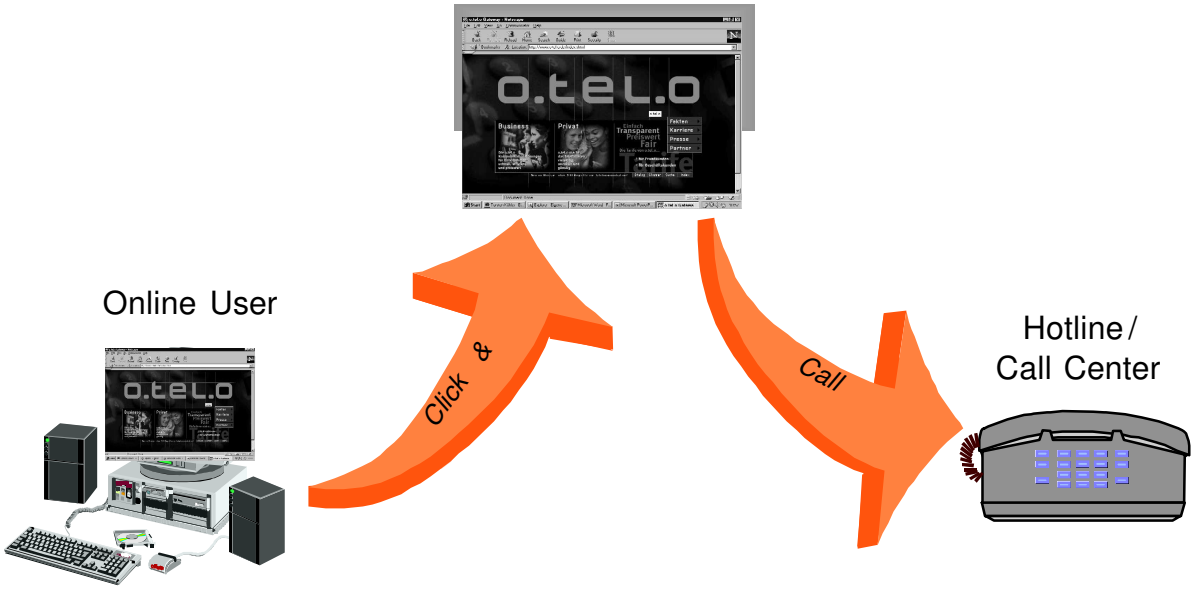


Potential II: Always Online



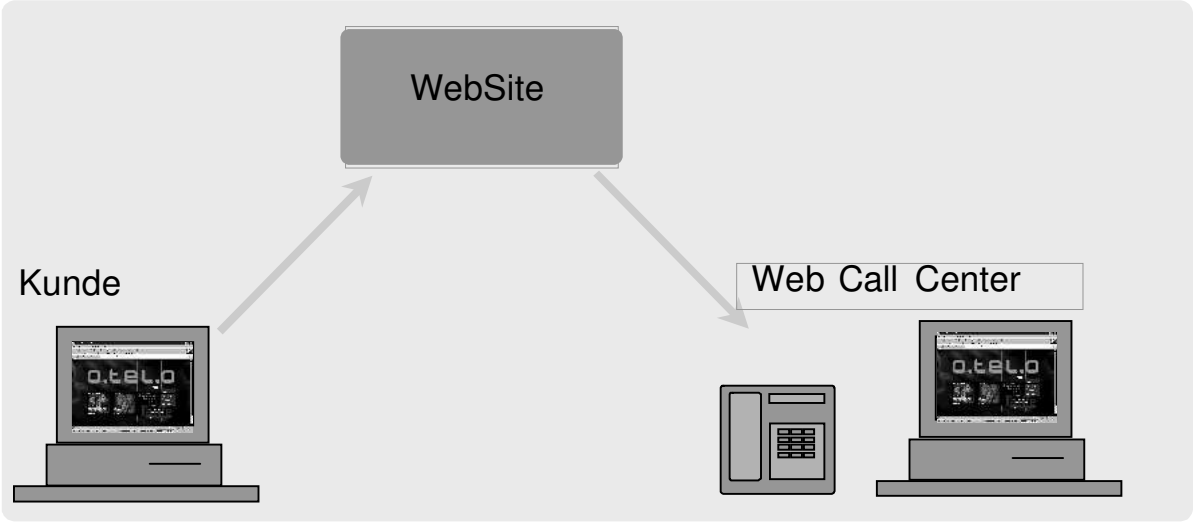
- Sprach-/Datenintegration auf einer Infrastruktur vor Ort
- Anschlußeinrichtung durch ISDN oder ADSL oder Kabelmodem
- Möglichkeiten für
  - nutzungsabhängiges Billing (Byte statt Minuten) zur Gebührenreduktion
  - günstige Mehrwertdienste wie MailBox, FaxBox, VoiceBox, InfoTerminal
  - PBX-lose Zweigstellen
  - etc.

Potential III: Click & Call Services



- Wandlung von passiver Information (Web) hin zu aktiver Kommunikation
- Differenzierung von WebSite, Hotline, CallCenter verschwimmt
- Optimaler Einsatz bereits vorhandener Infrastruktur (WebSite / Provider)

Potential IV: Web-enabled CallCenter



- Optimal vorbereitete CallCenter-Agents
- Effiziente Kundenberatung und -betreuung
- Kundenbindung durch direkte Mensch-zu-Mensch-Kommunikation, Überwindung der Web-Anonymität